# Turing-equivalent automata using a fixed-size quantum memory[*]

Abuzer Yakaryılmaz[†]
University of Latvia, Faculty of Computing, Raina bulv. 19, Rīga, LV-1586, Latvia
abuzer@lu.lv

March 4, 2013

Keywords: quantum complexity theory, Turing-equivalence, space-bounded computation, interactive proof systems, Arthur-Merlin games, alternation, complexity classes, finite state automata

## Abstract

In this paper, we introduce a new public quantum interactive proof system and the first quantum alternating Turing machine: qAM proof system and qATM, respectively. Both are obtained from their classical counterparts (Arthur-Merlin proof system and alternating Turing machine, respectively,) by augmenting them with a fixed-size quantum register. We focus on space-bounded computation, and obtain the following surprising results: Both of them with constant-space are Turing-equivalent. More specifically, we show that for any Turing-recognizable language, there exists a constant-space weak-qAM system, (the nonmembers do not need to be rejected with high probability), and we show that any Turing-recognizable language can be recognized by a constant-space qATM even with one-way input head.

For strong proof systems, where the nonmembers must be rejected with high probability, we show that the known space-bounded classical private protocols can also be simulated by our public qAM system with the same space bound. Besides, we introduce a strong version of qATM: The qATM that must halt in every computation path. Then, we show that strong qATMs (similar to private ATMs) can simulate deterministic space with exponentially less space. This leads to shifting the deterministic space hierarchy exactly by one-level. The method behind the main results is a new public protocol cleverly using its fixed-size quantum register. Interestingly, the quantum part of this public protocol cannot be simulated by any space-bounded classical protocol in some cases.

[*] A preliminary report on some contents of this paper was [YS11a].

[†] The author was partially supported by FP7 FET-Open project QCS.

# 1 Introduction

Anne Condon, in her famous PhD thesis [Con89], introduced a general computational model, i.e. *probabilistic game automaton*, that unifies many important computational models and concepts: *Alternation* of Chandra, Kozen, and Stockmeyer [CKS81], *private alternation* of Reif [Rei84], *Arthur-Merlin games* of Babai [Bab85], *interactive proof systems* of Goldwasser, Micali, and Rackoff [GMR89], *game against nature* of Papadimitriou [Pap85], etc. In this framework, Arthur-Merlin (AM) proof systems and alternation are the "weakest", since both are the games with *complete information*. In this paper, we introduce two new games by augmenting these two models with a fixed-size[1] quantum register, namely *qAM* and *q-alternation*, respectively. We focus our attention to space-bounded computation, and obtain the following surprising results: Both new games with constant space are *Turing-equivalent*.

Interactive proof (IP) systems and AM proof systems were introduced by Goldwasser, Micali, and Rackoff [GMR85] and Babai [Bab85], respectively. In time-bounded computation, it was shown that the class of languages having a polynomial-time IP or AM system is identical to $\mathsf{PSPACE}$ [Sha92]. In space-bounded computation, IP systems are more powerful than AM systems for any space-bound [Con89, Con91, DS92], e.g. the class of languages having a logarithmic-space AM system is identical to $\mathsf{P}$, and the class of languages having a logarithmic-space IP system is a superset of $\mathsf{EXPTIME}$. It was also shown that [CL89] for any Turing-recognizable language, there exits a constant-space *weak*[2]-IP system.

There are many different definitions of quantum interactive proof (QIP) systems [Kni96, Kit99, Wat99a, AN02, MW05]. In time-bounded computation, similar to the classical case, the class of languages having a polynomial-time QIP system were shown to be identical to $\mathsf{PSPACE}$ [JJUW11]. In space-bounded computation, the only published work belongs to Nishimura and Yamakami [NY09]. Their results, unfortunately, are model-dependent, and so do not reflect the full power of QIP systems since they use some restricted quantum automaton models as the verifiers.

Our qAM proof system is the first public space-bounded QIP system, and we present the first non-trivial results on space-bounded QIP systems. We show how a fixed-size quantum register leads to unexpected increase in the computational power of a public proof system. Our main result on the qAM system is that there exists a constant-space weak-qAM protocol for any Turing-recognizable language. In the classical case, a similar result is known for constant-space weak private protocols [CL89]. However, our protocol is not only public but also has perfect-completeness. Our second result is that for any known $s(n)$ space-bounded private protocol, there exists an equivalent $s(n)$ space-bounded qAM protocol, where $s(n) \in O(1) \cup \Omega(\log(n))$ is space-constructible. Therefore, we can say that logarithmic-space is sufficient for qAM systems for any language in $\mathsf{EXPTIME}$.

Alternation was introduced independently by Chandra and Stockmeyer [CS76] and Kozen [Koz76] as a generalization of nondeterminism. It was shown that alternation shifts the deterministic hierarchy

$$\mathsf{L} \subseteq \mathsf{P} \subseteq \mathsf{PSPACE} \subseteq \mathsf{EXPTIME} \subseteq \mathsf{EXPSPACE}$$

by exactly one level [CKS81]. On the other hand, the class of languages recognized by alternating finite automata is still the regular languages [CKS81]. Reif [Rei84] introduced private alternation by assuming that universal player can hide some information from the existential player, and showed that private alternation shifts the deterministic space hierarchy

$$\mathsf{L} \subsetneq \mathsf{PSPACE} \subsetneq \mathsf{EXPSPACE}$$

[1] The size of the register does not depend on the length of the input.

[2] The verifier does not need to halt with high probability for the nonmembers of the corresponding language.

by exactly one level.

Our q-alternation is *the first definition* of alternation in the domain of quantum computation. Our main result on q-alternation is that one-way q-alternating finite automata can recognize any Turing-recognizable language. In the classical case, the class of languages recognized by any space-bounded (private) ATMs is a proper subset of decidable languages [Rei84]. Since q-alternating machines may not halt the computation in every path, we also introduce the strong version of q-alternation by forbidding infinite computations. Then, we show that strong q-alternation, similar to private alternation, shifts the deterministic space hierarchy by exactly one level.

## 2 Preliminaries

For any string $x$, $|x|$ is the length of $x$ and $x[j]$ is its $j^{th}$ symbol, where $1 \leq j \leq |x|$. "#" is the blank symbol. Moreover, we represent $O(1)$ with $\mathsf{1}$ and $O(\log(n))$ with $\mathsf{log}$.

We assume that the reader is familiar with deterministic, nondeterministic, and alternating Turing machines, (DTM, NTM, and ATM, respectively,)[3] and their time- and space-bounded complexity classes $\mathcal{X}\mathsf{TIME}$ and $\mathcal{X}\mathsf{SPACE}$, where $\mathcal{X}$ is "D", "N", and "A", respectively; and, the following standard classes:

- $\mathsf{P} = \cup_{k>0}\mathsf{DTIME}(\mathsf{n^k})$ and $\mathsf{EXPTIME} = \cup_{k>0}\mathsf{DTIME}(2^{\mathsf{O}(\mathsf{n^k})})$;
- $\mathsf{L} = \mathsf{DSPACE}(\mathsf{log})$, $\mathsf{PSPACE} = \cup_{k>0}\mathsf{DSPACE}(\mathsf{n^k})$, and $\mathsf{EXPSPACE} = \cup_{k>0}\mathsf{DSPACE}(2^{\mathsf{O}(\mathsf{n^k})})$;
- $\mathsf{AL} = \mathsf{ASPACE}(\mathsf{log})$ and $\mathsf{APSPACE} = \cup_{k>0}\mathsf{ASPACE}(\mathsf{n^k})$.

In the following part, we provide the necessary background, based on [DS92, Con93], for the proof systems. For a detailed survey on space-bounded interactive proof systems, we refer the reader to [Con93]. An interactive proof system (IPS) consists of a prover ($P$) and a verifier ($V$). The verifier is a (resource-bounded) probabilistic Turing machine having a read-only input tape, a read/write work tape, and a source of random bits. Each head has two-way access to its tape. The states of the verifier are partitioned into reading, communication, and halting (accepting or rejecting) states, and it has a special communication cell for communicating with the prover, where the capacity of the cell is finite.

The one-step transitions of the verifier can be described as follows. When in a reading state, the verifier firstly flips an unbiased coin and then determines its next configuration based on the symbol under the tape heads, the state, and the outcome of the coin flip. When in a communication symbol, The verifiers writes a symbol on the communication cell with respect to the current state. Then, in response, the prover writes a symbol in the cell. Based on the state and the symbol written by prover, the verifier defines the next state of the verifier.

The prover $P$ is specified by a prover transition function, which determines the response of the prover to the verifier based on the input and the verifier's communication history until then. Note that this function does not need to be *computable*.

For a given input $x$, the probability that $(P, V)$ accepts (rejects) $x$ is the cumulative accepting (rejecting) probabilities taken over all branches of the verifier. The prover-verifier pair $(P, V)$ is an IPS for $L$ with error probability $\epsilon < \frac{1}{2}$ if

1. for all $x \in L$, the probability that $(P, V)$ accepts $w$ is greater than $1 - \epsilon$,
2. for all $x \notin L$, and all provers $P^*$, the probability that $(P^*, V)$ rejects $x$ is greater than $1 - \epsilon$.

[3] We refer the reader to [Rei84] for the details of private ATMs although it is not necessary to follow the content.

These conditions are known as completeness and soundness, respectively. Now, we define some variants of IP systems by restricting and/or relaxing the above conditions.

The prover-verifier pair $(P, V)$ is an *weak-IPS for $L$ with error probability $\epsilon < \frac{1}{2}$* if we relax the soundness condition (2) as follows:

$2'$. for all $x \notin L$, and all provers $P^*$, the probability that $(P^*, V)$ accepts $x$ is at most $\epsilon$.

The prover-verifier pair $(P, V)$ is a *(weak or not) IPS having perfect completeness* for $L$ if we restrict the completeness condition (1) as follows:

$1'$. for all $x \in L$, the probability that $(P, V)$ accepts $x$ is exactly equal to 1.

An Arthur-Merlin (AM) proof system (or a public-coin IPS) is a special case of IPS such that after each coin toss, the outcome is automatically written on the communication cell, and so the prover can have complete information about the computation of the verifier.

We will use $\mathsf{IP}(\cdot)$ and $\mathsf{AM}(\cdot)$ to represent the space-bounded complexity classes for IP and AM systems, respectively. Note that the space bound is always defined on the verifiers. The ones having perfect-completeness will be shown by $\mathsf{IP_1}(\cdot)$ and $\mathsf{AM_1}(\cdot)$, respectively. We will use prefix "weak-" to represent their "weak" versions.

Some known facts, related to our results, on AM and IP systems as given below. (We also refer the reader to Appendix A for the details of some private protocols.)

**Fact 1.** *[CL88, Con89, DS92] For any space-constructible $s(n) = \Omega(\log n)$,*

$$\mathsf{weak\text{-}AM(s(n))} = \mathsf{AM(s(n))} = \mathsf{ASPACE(s(n))}.$$

*Moreover,* $\mathsf{weak\text{-}AM(1)} \subsetneq \mathsf{weak\text{-}AM(log)} = \mathsf{AM(log)} = \mathsf{P}$.

**Fact 2.** *[CL89] Any Turing recognizable language is in* $\mathsf{weak\text{-}IP(1)}$.

**Fact 3.** *[DS92]* $\mathsf{DTIME(2^{O(n)})} = \mathsf{ASPACE(O(n))} \subseteq \mathsf{IP_1(1)}$.

**Fact 4.** *[Con89, CL89, DS92] For any space-constructible $s(n) = \Omega(\log(n))$,*

$$\mathsf{DTIME(2^{2^{O(s(n))}})} = \mathsf{ASPACE(2^{O(s(n))})} \subseteq \mathsf{IP_1(s(n))}.$$

**Fact 5.** *[CL89] For any space-constructible $s(n) = \Omega(\log(n))$,*

$$\mathsf{IP_1(s(n))} \subseteq \mathsf{IP(s(n))} \subseteq \mathsf{ATIME(2^{2^{2^{O(s(n))}}})}.$$

As seen from the above facts, private protocols are more powerful than public ones under the same space bounds. In case of weak-soundness, the power of the private protocols with finite-state verifiers becomes Turing-equivalent, which is never possible for a public protocol with any given space bound.

We will shortly show that the public protocols using a fixed-size quantum register can also implement some private protocols under the same space bounds. More specifically, the results presented in Facts 3 and 4 can also be obtained for qAM systems. Moreover, in case of weak-soundness, our new public protocol can also be Turing-equivalent even restricting to perfect-completeness, which can never be a case for private protocols with any given space bound due to Theorem 1 (see below).

**Theorem 1.** *For any space-constructible $s(n) \in \Omega(\log(n))$,*

$$\mathsf{IP_1(s(n))} \subseteq \mathsf{weak\text{-}IP_1(s(n))} \subseteq \mathsf{ASPACE(2^{2^{O(s(n))}})}.$$

*Proof.* See Appendix B. □

Note that Theorem 1 improves the previously known upper bound (Fact 5) for space-bounded IPS with perfect-completeness.

# 3 qAM

In this section, we give the definition of our new AM system (qAM) and present our results on qAM proof systems.

A qAM (*q*uantum Arthur-Merlin)[4] proof system is an AM system where the verifier additionally has a fixed size quantum register. The reading state of the new verifier is as follows:

> A superoperator, determined by the current state and the symbol(s) under the tape head(s), is applied to the quantum register, and the outcome of the operator is automatically written on the communication cell in order to satisfy *the complete information requirement*. Then, the next configuration is determined based on the the current state, the symbol(s) under the tape head(s), and the observed outcome. For any deterministic transition, the verifier applies an identity operator on the register. We refer the reader to Figure 1 for the details of superoperators.

Note that the verifier no longer needs a classical random source.[5] We will use $\mathsf{qAM}(\cdot)$ and $\mathsf{qAM_1}(\cdot)$ to represent qAM counterparts of $\mathsf{AM}(\cdot)$ and $\mathsf{AM_1}(\cdot)$, respectively. Prefix "weak-" is also applicable to $\mathsf{qAM}(\cdot)$ and $\mathsf{qAM_1}(\cdot)$. We give a simple qAM protocol for the well-known NP-complete language `SUBSET-SUM` in Appendix C.

The most general quantum operator is a superoperator, which generalizes stochastic and unitary operators and also includes measurement. Formally, a superoperator $\mathcal{E}$ is composed by a finite number of operation elements, $\mathcal{E} = \{E_1, \ldots, E_k\}$, satisfying that

$$\sum_{i=1}^{k} E_i^\dagger E_i = I, \tag{1}$$

where $k \in \mathbb{Z}^+$ and the indices are the measurement outcomes. When a superoperator, say $\mathcal{E}$, is applied to the quantum register in state $|\psi\rangle$, i.e. $\mathcal{E}(|\psi\rangle)$, we obtain the measurement outcome $i$ with probability $p_i = \langle\widetilde{\psi_i}|\widetilde{\psi_i}\rangle$, where $|\widetilde{\psi_i}\rangle$, *the unconditional state vector*, is calculated as $|\widetilde{\psi_i}\rangle = E_i|\psi\rangle$ and $1 \leq i \leq k$. (Note that using unconditional state vector simplifies calculations in many cases.) If the outcome $i$ is observed ($p_i > 0$), the new state of the system is obtained by normalizing $|\widetilde{\psi_i}\rangle$, which is $|\psi_i\rangle = \frac{|\widetilde{\psi_i}\rangle}{\sqrt{p_i}}$. Moreover, as a special operator, the quantum register can be initialized to a predefined quantum state. This initialize operator, which has only one outcome, is denoted $\acute{\mathcal{E}}$. In this paper, the entries of quantum operators are defined by rational numbers. Thus the probabilities of the outcomes are always rational numbers.

Figure 1: The details of superoperators

Knowledgeable readers will have noticed that, when the verifier is restricted to use constant space, the qAM system is actually the quantum counterpart of the finite automaton with both nondeterministic and probabilistic states of Condon et. al. [CHPW98], and that if we remove the communication with the prover as well we end up with a finite automaton with quantum and classical states (2QCFA) of Ambainis and Watrous [AW02].

In our qAM protocols (and later in our q-alternation simulations), we use some non-unitary transformations to implement our main tasks. We define our superoperators based on these transformations. Let $E_1, \ldots, E_k$ be some of these transformations. We can obtain a superoperator $\mathcal{E}$ based on them by defining some additional transformations $E_{k+1}, \ldots, E_{k+k'}$ such that

$$\mathcal{E} = \left\{ \frac{1}{d}E_1, \ldots, \frac{1}{d}E_k, \frac{1}{d}E_{k+1}, \ldots, \frac{1}{d}E_{k+k'} \right\}$$

[4] The small "q" indicates that the verifier has a "very small" (possible the smallest) quantum resource.

[5] For example, the superoperator $\mathcal{E} = \left\{E_{h_1} = \frac{1}{2}I, E_{h_2} = \frac{1}{2}I, E_{t_1} = \frac{1}{2}I, E_{t_2} = \frac{1}{2}I\right\}$ always produces the outcomes *head* ("$h_1$" or "$h_2$) and *tail* ("$t_1$" or "$t_2$") with probability $\frac{1}{2}$.

satisfies Condition 1 in Figure 1 for a convenient $d > 1$, where $k' > 0$.[6] We call $\left\{\frac{1}{d}E_1, \ldots, \frac{1}{d}E_k\right\}$ *the main operation elements* and $\left\{\frac{1}{d}E_{k+1}, \ldots, \frac{1}{d}E_{k+k'}\right\}$ *the auxiliary operation elements*. Moreover, in our protocols, the computation continues on the quantum register only when the outcomes of some main operation elements are observed. On the other hand, the current computation on the quantum register is always terminated/restarted with discarding the current content of the register when the outcome of an auxiliary operation element is observed. Therefore, the details of the auxiliary operation elements can be omitted from the description of the protocols.

In the following part, we present our qAM protocols. We begin with a constant-space weak-qAM protocol having perfect completeness for any given Turing-recognizable language. We present our result by giving *a new public protocol* simulating a given DTM. Contrary to the classical case,[7] our simulation technique can also be applicable to the case of strong-soundness. Therefore, after making certain modifications, we present our other space-bounded qAM protocols. Note that, all of our qAM protocols have *perfect-completeness*.[8] Interestingly, this property allows us to use the same techniques for q-alternation after making some restrictions and modifications.

**Theorem 2.** *Any Turing recognizable language is in* $\mathsf{weak\text{-}qAM_1}(1)$*.*

*Proof.* Let $\mathtt{L}$ be a Turing recognizable language and $\mathcal{D}$ be a single-tape DTM recognizing $\mathtt{L}$. We will construct a weak-qAM proof system $(P, V)$ for $\mathtt{L}$ with perfect completeness, where $V$ is a finite state verifier.

We begin with some details of $\mathcal{D}$. $Q$ containing $q_1$ (the initial state), $q_a$ (the accepting state), and $q_r$ (the rejecting state) is the set of states, $\Gamma$ containing $\#$ is the tape alphabet, and $\Gamma' = Q \cup \Gamma$, called configuration alphabet, where $Q$ and $\Gamma$ are disjoint sets and $\$ \notin \Gamma$. Note that $\Gamma'$ contains at least 5 elements. Any configuration of $\mathcal{D}$ is of the form $uqv$ ($\mathcal{D}$ is in $q$ and the tape head is on the leftmost symbol of $v$), where $q \in Q$ and $uv \in \#(\Gamma)^*\#$. The unnecessary blank symbols are always dropped from the descriptions of configurations. For a given input string $x$, the initial configuration is represented as $q_1\#x\#$.

The main protocol is executed in an infinite loop and each iteration (round) is composed by the following: (i) The verifier requests the computation (a sequence of configurations starting from the initial configuration) of $\mathcal{D}$ on the given input, say $x$, from the prover. (ii) Against the cheating provers, the verifier checks the correctness of the computation and rejects $x$ if it detects a defect in the computation. (iii) When it encounters a halting configuration, the verifier mimics the decision of this (halting) configuration.

Let $w$ be the string obtained from the prover in a single round. The verifier expects $w$ as $c_1\$\$c_2\$\$c_3\$\$\cdots$, where (P1) $c_i$'s ($i > 0$) are some configurations of $\mathcal{D}$, (P2) $c_1$ is the initial configuration, and (P3) $c_{i+1}$ is the successor of $c_i$ in one step for any $i > 0$. (We use double \$ for pedagogical reasons.) Note that $w$ can be an infinite string. The verifier can check P1 and P2 deterministically, and $x$ is rejected immediately if one of them fails. Therefore, in the following part, we assume that $w$ satisfies both P1 and P2 and each configuration ends with "\$\$".

The non-trivial part is to check P3 for each $i > 0$, i.e. whether $c_{i+1}$ is identical to $\mathtt{next}(c_i)$, where $\mathtt{next}(c_i)$ is the single-step successor of $c_i$. This is where the quantum register comes into play. The idea behind is to encode $\mathtt{next}(c_i)$ and $c_{i+1}$ into the amplitudes of two states on the register, and then to subtract them, and to reject $x$ with the resulting amplitude.[9] We call this procedure

[6] We refer the reader [YS10, YS11b] for similar procedures.

[7] In classical case, to show universality of constant-space weak-IP systems, a simulation of two-way finite automaton with two-counters was given [CL89]. Since the complexity classes are defined by Turing machines, this technique does not seem to be applicable to the case of strong-soundness. (See also Appendix A)

[8] Two-sided bounded error is necessary for the universality of constant-space weak-IP systems due to Theorem 1.

[9] In fact, the encoding part can also be implemented by a probabilistic system but the aforementioned *subtraction* is not possible in classical systems!

*successor-check*. The $i^{th}$ successor-check compares $\texttt{next}(c_i)$ and $c_{i+1}$. As will be detailed below, whenever $c_{i+1} = \texttt{next}(c_i)$ (for all defined $i > 0$), the input is never rejected by a successor-check. Thus, once a halting configuration is obtained from the prover, the *only decision* is made based on it. Otherwise, i.e. $\exists i > 0$ s.t. $c_{i+1} \neq \texttt{next}(c_i)$, $x$ is rejected by the $i^{th}$ successor-check. We show that such a reject probability is sufficiently greater than any accept probability in a single round.

In the remaining part, we will give the details of a single round and the analyses of the protocol. The verifier requests the computation of $\mathcal{D}$ on $x$ symbol by symbol from the prover, and it uses a 3-symbol buffer to parallelly encode the legal successor of the presently scanned configuration. The verifier uses a 4-state quantum register, $q_1, \ldots, q_4$, which is set to $|\psi_{1,0}\rangle = (1 \quad 0 \quad 0 \quad 0)^T$ at the beginning of each round. The configurations are encoded in base-$m$, where $m = |\Gamma'| + 1$. Each symbol of $\Gamma'$ is associated with a different positive integer. Thus, any configuration $c_i$ $(i > 0)$ can be represented by a $|c_i|$-length number in base-$m$. We use the same symbol for both the encoded string/symbol and its encoding. The verifier applies one superoperator per symbol. When the outcome of an auxiliary operation elements is observed, the verifier terminates the current round and initiates a new round. The tasks implemented by the main operation elements reduce the amplitudes with $\frac{1}{d} < 1$. Therefore, after applying each superoperator, a new round is initiated with some probability. In other words, a round can continue only with a small probability. The complete details of the superoperators and the related operations are given at the end of the proof due to their technicalities.

Let $l_i$ be the length of $c_1\$\$c_2\$\$ \cdots c_i\$\$$ $(i > 0)$. By processing $c_1\$\$$, i.e. a series of superoperators $\mathcal{E}_{1,1}, \ldots, \mathcal{E}_{1,|c_1\$\$|}$ are applied to the register, $\texttt{next}(c_1)$ is encoded into the amplitudes of $|q_2\rangle$. Then, the quantum state becomes[10]

$$|\widetilde{\psi_{2,0}}\rangle = \left(\frac{1}{d}\right)^{l_1} \begin{pmatrix} 1 \\ \texttt{next}(c_1) \\ 0 \\ 0 \end{pmatrix}.$$

Similarly, by processing $c_2\$$, $c_2$ and $\texttt{next}(c_2)$ are encoded into the amplitudes of $|q_3\rangle$ and $|q_4\rangle$, respectively:

$$|\widetilde{\psi_{2,|c_2\$|}}\rangle = \left(\frac{1}{d}\right)^{l_2-1} \begin{pmatrix} 1 \\ \texttt{next}(c_1) \\ c_2 \\ \texttt{next}(c_2) \end{pmatrix}.$$

After processing one more \$, the first successor-check is finalized: The corresponding superoperator has two main operation elements. The first one is responsible for comparing $\texttt{next}(c_1)$ and $c_2$, and subtracts the amplitudes of $|q_2\rangle$ and $|q_3\rangle$. Its outcome is observed with probability

$$\left(\frac{1}{d}\right)^{2l_2} (\texttt{next}(c_1) - c_2)^2,$$

which is also the rejecting probability of the first successor-check. The second main operation element is determined conditionally. If $\texttt{next}(c_2)$ is an accepting (a rejecting) configuration, then it selects only the amplitude of $|q_1\rangle$, the outcome of which is observed with probability $\left(\frac{1}{d}\right)^{2l_2}$. This probability is also the accepting (rejecting) probability of the round. Since the computation is terminated due to the outcomes of both operation elements, the round does not continue in this

[10] Note that, unconditional state vectors facilitate the calculations. The probabilities can be calculated directly.

case. If $\texttt{next}(c_2)$ is not a halting configuration, the round continues with the next successor-check. Thus the quantum state becomes

$$|\widetilde{\psi_{3,0}}\rangle = \left(\frac{1}{d}\right)^{l_2} \begin{pmatrix} 1 \\ \texttt{next}(c_2) \\ 0 \\ 0 \end{pmatrix}.$$

One can easily verify that if the prover is cheating about $c_2$, the input is rejected with a probability at least $m^2 \left(\frac{1}{d}\right)^{2l_2}$ since both $\texttt{next}(c_1)$ and $c_2$ end with a # and they must be disagree on at least one digit. If the prover is honest, the decision is given only if $\texttt{next}(c_2)$ is a halting configuration, whose probability is at least $m^2$ smaller than the above rejecting probability. The other successor-checks are executed exactly in the same way (see the end of the proof).

The analysis of the protocol is as follows. If $x \in L$, then $P$ always sends the correct computation of $\mathcal{D}$ on $x$ to $V$, say $c_1\$\$c_2\$\$\cdots\$\$c_t\$\$$ such that $\texttt{next}(c_t)$ is an accepting configuration. Then $V$ never rejects but accepts $x$ with probability $\left(\frac{1}{d}\right)^{2l_t}$ in each round. So, $x$ is accepted exactly by $V$.

If $x \notin L$, then the only case in which $V$ accepts $x$ is that $P^*$ send a computation of some nonhalting configurations $c_1\$\$c_2\$\$\cdots\$\$c_{t'}\$\$$ such that $\texttt{next}(c_{t'})$ is an accepting configuration, where $t' > 1$. Since $x \notin L$, there must be an $i$ $(1 \leq i < t')$ such that $\texttt{next}(c_i) \neq c_{i+1}$. Therefore, $x$ is rejected with probability at least $m^2$ times greater than the accepting probability in a single round. In other words, the overall accepting probability can be bounded above by $\frac{1}{m^2+1}$. This bound can be easily reduced to any desired value by selecting a greater $m$ value.

Now, we give the omitted details of the superoperators and the related operations below. Remember that $l_i$ is the length of $c_1\$\$c_2\$\$\cdots c_i\$\$$ and the quantum state is set to

$$|\psi_{1,0}\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

at the beginning of each round. As described before, we omit the details of each auxiliary operation element, and a new round is initiated when the outcome of such an operation element is observed.

For each symbol of $w_1 = c_1\$\$$, the verifier applies $|w_1|$ superoperators, $\mathcal{E}_{1,1}, \ldots, \mathcal{E}_{1,|w_1|}$, to the register, some of the the same. The aim is to encode $\texttt{next}(c_1)$ into the amplitudes of $|q_2\rangle$. For each $j \in \{1, \ldots, |c_1| - 1\}$, the main operation element of $\mathcal{E}_{1,j}$ is as follows:

$$\frac{1}{d} \begin{pmatrix} 1 & 0 & 0 & 0 \\ \texttt{next}(c_1)[j] & m & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

For $\mathcal{E}_{1,|c_1|}$ and $\mathcal{E}_{1,|c_1\$|}$, we have the following cases, each of which can be deterministically determined and handled by using 3-symbol buffer:

- If $|\texttt{next}(c_1)| = |c_1| - 1$, the main operation elements of $\mathcal{E}_{1,|c_1|}$ and $\mathcal{E}_{1,|c_1\$|}$ are as follows:

$$\frac{1}{d} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \text{ and } \frac{1}{d} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix},$$

respectively, since the encoding of $\texttt{next}(c_1)$ is finished by superoperator $\mathcal{E}_{1,|c_1|-1}$.

- If $|\texttt{next}(c_1)| = |c_1|$, the main operation elements of $\mathcal{E}_{1,|c_1|}$ and $\mathcal{E}_{1,|c_1\$|}$ are as follows:

$$\frac{1}{d}\begin{pmatrix} 1 & 0 & 0 & 0 \\ \# & m & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \text{ and } \frac{1}{d}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix},$$

respectively, since the encoding of $\texttt{next}(c_1)$ is finished by superoperator $\mathcal{E}_{1,|c_1|}$. (Note that the last symbol of any configuration is a blank symbol.)

- If $|\texttt{next}(c_1)| = |c_1| + 1$, the main operation elements of $\mathcal{E}_{1,|c_1|}$ and $\mathcal{E}_{1,|c_1\$|}$ are as follows:

$$\frac{1}{d}\begin{pmatrix} 1 & 0 & 0 & 0 \\ \texttt{next}(c_1)[|c_1|] & m & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \text{ and } \frac{1}{d}\begin{pmatrix} 1 & 0 & 0 & 0 \\ \# & m & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix},$$

respectively, since the encoding of $\texttt{next}(c_1)$ is finished by superoperator $\mathcal{E}_{1,|c_1|+1}$.

The main operation elements of $\mathcal{E}_{1,|c_1\$\$|}$ is as follows:

$$\frac{1}{d}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Thus, after applying superoperators $\mathcal{E}_{1,j}$'s ($1 \leq j \leq |w_1|$), the state vector of the register becomes

$$|\widetilde{\psi_{2,0}}\rangle = \left(\frac{1}{d}\right)^{l_1} \begin{pmatrix} 1 \\ \texttt{next}(c_1) \\ 0 \\ 0 \end{pmatrix}. \tag{2}$$

We continue with the block $w_2 = c_2\$\$$. In fact, the tasks implemented in this part are the same for any other block $w_i = c_i\$\$$ ($i > 2$). Similar to the above case, for each symbol of $w_2$, the verifier applies $|w_2|$ superoperators, $\mathcal{E}_{2,1}, \ldots, \mathcal{E}_{2,|w_2|}$, to the register, some of which can be the same. Remember that before starting to apply any operator, the unconditional state vector is $|\widetilde{\psi_{2,0}}\rangle$ (Equation 2). The aims in this block ($w_2$) are as follows:

1. By processing $c_2\$$,
   (a) to encode $c_2$ into the amplitudes of $|q_3\rangle$ and
   (b) to encode $\texttt{next}(c_2)$ into the amplitudes of $|q_4\rangle$.
2. By processing the second \$,
   (a) to finalize the $1^{st}$ successor-check,
   (b) to accept or reject the input if $\texttt{next}(c_2)$ is an accepting or a rejecting configuration, respectively; and, to start $3^{rd}$ successor-check if $\texttt{next}(c_2)$ is not a halting configuration.

The details of superoperators to encode $c_2$ and $\texttt{next}(c_2)$ are similar to the ones given above. For each $j \in \{1, \ldots, |c_2| - 1\}$, the main operation element of $\mathcal{E}_{2,j}$ is as follows:

$$\frac{1}{d}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ c_2[j] & 0 & m & 0 \\ \texttt{next}(c_2)[j] & 0 & 0 & m \end{pmatrix}.$$

For $\mathcal{E}_{2,|c_2|}$ and $\mathcal{E}_{2,|c_2\$|}$, we have the following cases:

- If $|\texttt{next}(c_2)| = |c_2| - 1$, the main operation elements of $\mathcal{E}_{2,|c_2|}$ and $\mathcal{E}_{2,|c_2\$|}$ are as follows:

$$\frac{1}{d}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ \# & 0 & m & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \text{ and } \frac{1}{d}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

respectively, since the encoding of $\texttt{next}(c_2)$ is finished by the superoperator $\mathcal{E}_{2,|c_2|-1}$.

- If $|\texttt{next}(c_2)| = |c_2|$, the main operation elements of $\mathcal{E}_{2,|c_2|}$ and $\mathcal{E}_{2,|c_2\$|}$ are as follows:

$$\frac{1}{d}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ \# & 0 & m & 0 \\ \# & 0 & 0 & m \end{pmatrix} \text{ and } \frac{1}{d}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

respectively, since the encoding of $\texttt{next}(c_2)$ is finished by the superoperator $\mathcal{E}_{2,|c_2|}$.

- If $|\texttt{next}(c_2)| = |c_2| + 1$, the main operation elements of $\mathcal{E}_{2,|c_2|}$ and $\mathcal{E}_{2,|c_2\$|}$ are as follows:

$$\frac{1}{d}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ \# & 0 & m & 0 \\ \texttt{next}(c_2)[|c_2|] & 0 & 0 & m \end{pmatrix} \text{ and } \frac{1}{d}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ \# & 0 & 0 & m \end{pmatrix},$$

respectively, since the encoding of $\texttt{next}(c_2)$ is finished by superoperator $\mathcal{E}_{2,|c_2|+1}$.

Thus, before applying $\mathcal{E}_{2,|c_2\$\$|}$, the state vector becomes as follows:

$$|\widetilde{\psi_{2,|c_2\$|}}\rangle = \left(\frac{1}{d}\right)^{l_2-1}\begin{pmatrix} 1 \\ \texttt{next}(c_1) \\ c_2 \\ \texttt{next}(c_2) \end{pmatrix}. \tag{3}$$

Operator $\mathcal{E}_{2,|c_2\$\$|}$ has two main operation elements. This first one is responsible to finalize the $1^{th}$ successor-check:

$$\frac{1}{d}\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

The associated action of this operation element is *to reject the input.* Therefore, the input is rejected with probability

$$\left(\frac{1}{d}\right)^{2l_2}(\mathtt{next}(c_1)-c_2)^2,$$

which is zero if the check succeeds ($\mathtt{next}(c_1)=c_2$) and is at least

$$\left(\frac{1}{d}\right)^{2l_2}m^2$$

if the check fails ($\mathtt{next}(c_1)\neq c_2$). Since the last symbol of $\mathtt{next}(c_1)$ and $c_2$ are the identical, the value of $|\mathtt{next}(c_1)-c_2|$ can be at least $m$.

The second main operation element is determined by the type of $\mathtt{next}(c_2)$:

- If it is an accepting (a rejecting) configuration, then the following operation element is applied:

  $$\frac{1}{d}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

  The associated action of this is *to accept (reject) the input.* Therefore, the input is accepted (rejected) with probability

  $$\left(\frac{1}{d}\right)^{2l_2}.$$

  Note that the round is certainly terminated in this case.

- If it is not a halting configuration, then the following operation element is applied:

  $$\frac{1}{d}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

  The associated action of this is to continue the round, and so *to initiate* the $3^{rd}$ successor-check. The state vector becomes

  $$|\widetilde{\psi_{3,0}}\rangle=\left(\frac{1}{d}\right)^{l_2}\begin{pmatrix} 1 \\ \mathtt{next}(c_2) \\ 0 \\ 0 \end{pmatrix}.$$

Note that if the prover never sends $\$\$$ symbols, then no decision is given.

The tasks for block $w_3=c_3\$\$$ is exactly the same as for block $w_2=c_2\$\$$, and the tasks for block $w_4=c_4\$\$$ is exactly the same as for block $w_3=c_3\$\$$, and so on. Therefore we can generalize it for a generic block $w_i=c_i\$\$$, where $i\geq 2$. The state vector is

$$|\widetilde{\psi_{i,0}}\rangle=\left(\frac{1}{d}\right)^{l_{i-1}}\begin{pmatrix} 1 \\ \mathtt{next}(c_{i-1}) \\ 0 \\ 0 \end{pmatrix}$$

at the beginning. The aims are as follows:

1. By processing $c_i\$$,
    (a) to encode $c_i$ into the amplitudes of $|q_3\rangle$ and
    (b) to encode $\texttt{next}(c_i)$ into the amplitudes of $|q_4\rangle$.
2. By processing the second \$,
    (a) to finalize the $(i-1)^{st}$ successor-check,
    (b) to accept or reject the input if $\texttt{next}(c_i)$ is an accepting or a rejecting configuration, respectively; and, to start the $(i+1)^{st}$ successor-check if $\texttt{next}(c_i)$ is not a halting configuration.

When the $(i-1)^{st}$ successor-check is finalized, the input is rejected with probability

$$\left(\frac{1}{d}\right)^{2l_i} (\texttt{next}(c_{i-1}) - c_i)^2,$$

which can be at least

$$\left(\frac{1}{d}\right)^{2l_i} m^2$$

if $\texttt{next}(c_{i-1}) \neq c_i$. If $\texttt{next}(c_i)$ is an accepting (a rejecting) configuration, then the input is accepted (rejected) with probability

$$\left(\frac{1}{d}\right)^{2l_i}.$$

Otherwise, the $(i+1)^{st}$ successor-check initialized with the state vector

$$|\widetilde{\psi_{i,0}}\rangle = \left(\frac{1}{d}\right)^{l_i} \begin{pmatrix} 1 \\ \texttt{next}(c_i) \\ 0 \\ 0 \end{pmatrix}.$$

□

One of the remarkable properties of our protocol is that the quantum register can be in a *superposition* of two successor-checks, which is one of the fundamental and distinctive properties of quantum computation. In fact, classical private protocols can also "imitate" this phenomenon: The verifier privately selects odd- or even-numbered successor-checks, and so, *from the viewpoint of the prover*, the verifier seems to be in a superposition of two successor-checks (such as, with probability $\frac{1}{2}$). However, in our protocol, the verifier *really* is in a superposition and it is independent from any prover. This is indeed why our protocol works in a public setting. Therefore, our protocol can be seen as a new and elegant evidence on how the superposition phenomenon can become useful in terms of complexity theory.

The main consequence of Theorem 2 is that qAM systems can be more powerful than IP systems:

**Corollary 1.** *For any space bound $s(n)$,* $\mathsf{weak\text{-}IP_1(s(n))} \subsetneq \mathsf{weak\text{-}qAM_1(1)}$.

Now, we turn our attention to the protocols in which the computation always halts with high probability. (Note that, our weak-protocol may run forever in some cases, i.e., the simulated machine may run forever on the given input, a cheating prover never sends \$\$ after sending a few valid configurations, etc.) In our weak-protocol (above), the input head of the verifier is never used after checking the first configuration. In fact, it can be used to check whether the length of a configuration sent by the prover is linear. Thus, the verifier can force the prover to send linear-size configurations. So, it can be easily obtained that $\mathsf{DSPACE(n)} \subseteq \mathsf{qAM_1(1)}$, i.e. the prover sends the computation of a linear-space DTM. If the prover is additionally asked to provide nondeterministic choices, this result is extended to that $\mathsf{NSPACE(n)} \subseteq \mathsf{qAM_1(1)}$, i.e. the prover sends the computation of a linear-space NTM, in which nondeterministic choices are determined by the prover. Although it is not trivial as the above two results, we can go one further step: $\mathsf{ASPACE(n)} \subseteq \mathsf{qAM_1(1)}$, i.e. the prover sends the computation of a linear-space ATM, in which nondeterministic choices are determined by the prover and universal choices are determined by the verifier. This idea was firstly given by Reif [Rei84] for the simulation of a space-bounded ATM by a private ATM, and then used by Condon and Ladner [CL88], Condon [Con89], and Dwork and Stockmeyer [DS92] for similar simulations. We follow the latest result by embedding the simulation idea of Dwork and Stockmeyer [DS92] into our weak-protocol by making some modifications.

**Theorem 3.** $\mathsf{DTIME}(2^{\mathsf{O(n)}}) = \mathsf{ASPACE(n)} \subseteq \mathsf{qAM_1(1)}$.

*Proof.* Let $\mathtt{L}$ be a language in $\mathsf{ASPACE(n)}$. Then, there exists a single-tape ATM $\mathcal{A}$ recognizing $\mathtt{L}$. The components of $\mathcal{A}$ is similar to $\mathcal{D}$ given in the proof of Theorem 2. (Note that, for an ATM, any nonhalting state is labelled as either existential or universal.) We make some additional assumptions on $\mathcal{A}$ as given in Dwork and Stockmeyer [DS92] (See also Appendix A). Tape alphabet $\Gamma$, apart from $\#$, contains another special symbol $¢$. The input, say $x$, is given as $¢x¢$, $¢$ is only overwritten by $¢$, the head is not allowed to leave the area between the cent symbols, and any non-cent symbol is only overwritten by a non-cent symbol. Thus, any configuration of $\mathcal{A}$ is of the form $uqv$ such that $q \in Q$ and $uv \in ¢(\Gamma \setminus \{¢\})^{|x|}¢$. We assume that $\mathcal{A}$ makes an existential move after a universal one and vice versa. Moreover, each such a transition leads to exactly two branches. In order to fix the running time in each branch, we assume that $\mathcal{A}$ has some additional deterministic states (i.e. universal states with no branching) to keep a counter to guarantee that the decision is always given after making $2^{c|x|}$ branching transitions. So, we can group non-halting states of $\mathcal{A}$ into three groups:

1. existential states,
2. universal states leading to two transitions, and
3. universal states leading to one transition.

The third ones are called deterministic states to prevent confusion. So, the second ones are called just universal states. We also assume that each counter operation takes the same amount of steps, which is only dependent on the length of input ($|x|$). So the computation tree of $\mathcal{A}'$ on $x$, denoted by $\mathcal{T}_{\mathcal{A}}(x)$, has $2^{2^{c|x|}}$ leafs, and each path from the root to a leaf has the same depth, where $c$ is an appropriate constant. If the leaf is an accepting (rejecting) configuration, then the path is called accepting (rejecting) path.

Now we will describe a qAM proof system $(P, V)$ for $\mathtt{L}$ with perfect completeness based the qAM system given in the proof of Theorem 2 after making some modifications, where $V$ is a finite state verifier.

The first modification is that the verifier requests a computation path of $\mathcal{T}_{\mathcal{A}}(x)$, i.e. a path from the root to one of the leafs, from the prover in each round. The format of the computation is the same:

$$c_1\$\$c_2\$\$\cdots c_i\$\$c_{i+1}\$\$\cdots .$$

However, before a successor-check, say the $i^{th}$ one, the verifier should know which branch it follows after $c_i$ since the verifier encodes $\texttt{next}(c_i)$ during processing $c_i\$\$$. Therefore, the verifier should know the follow-up branch before obtaining $c_i\$\$$. Similarly, the prover should be aware of this branch before sending $c_{i+1}$. As mentioned earlier, any existential branch is determined by the prover and any universal branch is determined by the verifier. One of the convenient way is that before communicating on $c_i\$\$$, both parties exchange their decisions *about which branch is followed after* $c_i$. Remark that if $c_i$ is a deterministic branch, then both choices become useless, if it is an existential (a universal) one, the choice of the prover (the verifier) becomes useless. The verifier makes its choice with equal probability. Therefore, it applies a superoperator having the following two main operation elements

$$\left\{ \underbrace{\frac{1}{d}I}_{l}, \underbrace{\frac{1}{d}I}_{r} \right\},$$

where outcome "l" ("r") represents the left-branch (right-branch) and $I$ is the identity operator.

The second modification is that each configuration length is *deterministically* checked by the verifier to be equal to $|x| + 2$ by help of the input head. (We denote this property as P4.) If not, the computation is terminated and the input is rejected immediately.

The third modification is about the acceptance probability, which is dramatically made smaller when compared to the one in the original protocol. We describe why the original strategy does not work with an example.

> Remember that if a round ends with an accepting (a rejecting) configuration in the original protocol, then the input is accepted (rejected) with a probability calculated by the amplitude of $|q_1\rangle$. Suppose that the prover sends a computation of $\mathcal{A}$ satisfying P1-P4. Then if the verifier follows the original strategy, the input is rejected (accepted) with the same probability at the end of each round since the length of each path is equal in this case. If the prover follows a nondeterministic strategy of $\mathcal{A}$ that leads to exactly one rejecting leaf, then the input is accepted with a high probability although the input must be rejected with high probability with respect to this subtree.

Our new acceptance strategy is as follows. The verifier uses an additional state, $q_5$, on the register. When a new round is initiated, the state vector is immediately set to

$$\left(\frac{1}{d}\right) \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}.$$

Then, the amplitude of $|q_5\rangle$ is multiplied by

$$\left(\frac{1}{2d}\right)$$

for each configuration in the computation. The input is accepted similar to the original protocol but by the amplitudes of $|q_5\rangle$. Note that after making $b$ branches, the ratio of the amplitude of $|q_1\rangle$ to the amplitude of $|q_5\rangle$ is $2^b$, and so, any rejecting probability calculated by the amplitude of $|q_1\rangle$ is $4^b$ times greater than any accepting probability calculated by the amplitude of $|q_1\rangle$.

Now, we can analyse our modified protocol. If $x \in L$, then (honest) $P$ always sends a valid computation of $\mathcal{A}$ on $x$, and the input is always accepted with a (constant) non-zero probability in each round. Therefore, $x$ is accepted by $V$ exactly.

If $x \notin L$, there exists always at least one rejecting path whichever nondeterministic strategy is followed. As known form the original protocol, if the prover ($P^*$) sends some configurations violating any of P1-P4, then the rejecting probability is always sufficiently greater than the accepting one in a single round. Therefore, suppose that the prover sends the configurations satisfying P1-P4. Let $p$ be the probability of rejecting $x$ at the end of a rejecting path. So, the accepting probability of $x$ at the end of an accepting path is equal to

$$p(\frac{1}{4})^{2^{c|x|}}.$$

Since there can be at most $2^{2^{c|x|}} - 1$ accepting paths, a single rejecting probability is sufficiently greater than the overall accepting probability. □

**Theorem 4.** *For any space-constructible $s(n) \in \Omega(\log(n))$,*

$$\mathsf{DTIME}(2^{2^{\mathsf{O(s(n))}}}) = \mathsf{ASPACE}(2^{\mathsf{O(s(n))}}) \subseteq \mathsf{qAM_1(s(n))}.$$

*Proof.* In this case, the verifier can force the prover to send $2^{O(s(n))}$-size configurations by using its classical work tape. The remainder follows from the proof of Theorem 3. □

**Corollary 2.** $\mathsf{EXPTIME} \subseteq \mathsf{qAM_1(log)}$.

Due to Fact 1 and Theorem 4, we can follow that qAM systems (having perfect-completeness) are *strictly* more powerful than any AM system under the same space bound.

**Corollary 3.** *For any space bound $s(n)$,*

$$\mathsf{AM(s(n))} \subseteq \mathsf{weak\text{-}AM(s(n))} \subsetneq \mathsf{qAM_1(s(n))}.$$

# 4 q-Alternation

As mentioned earlier, alternation and AM proof systems are games with *complete information.* Moreover, they could be obviously related to each other, e.g. alternation can be "inherited" from AM systems as follows: The verifier is replaced by a universal player and all provers are represented by an existential player.[11]

In this section, we introduce the notion of *quantum alternation for the first time.* We define quantum alternation similar to our qAM system, i.e., its quantum part is only a fixed-size quantum register and this register can only be accessible by the universal states. We call the model *q-alternation* due to its "very" limited quantum part, and give the definition based on Turing machine, *q-alternating Turing Machine* (qATM).

A qATM is an ATM augmented with a fixed-size quantum register, based on which universal branches are determined. Any configuration of a qATM can be represented by a pair $(c, |\psi\rangle)$, where $c$ represent the classical configuration of the machine and $|\psi\rangle$ is the state of quantum register. Let $\{c_1, \ldots, c_{k_c}\}$ be the transitions determined by the classical transition function of the machine with respect to the classical state and the symbol(s) under the tape head(s) in configuration $c$, where $k_c$

[11] We refer the reader to Condon [Con89] for the technical details.

is the total number branches. If $c$ is an existential configuration, then only the classical part of the qATM is changed, and the following transition(s) is (are) implemented:

$$(c, |\psi\rangle) \to \{(c_i, |\psi\rangle) \mid 1 \leq i \leq k_c\}.$$

If $c$ is a universal configuration, then both the classical part and the quantum state of the qATM are changed: The machine applies a superoperator determined by the classical state and the symbol(s) under the tape head(s) in configuration $c$, $\mathcal{E}_c = \{E_{c,1}, \ldots, E_{c,k_c}\}$, to the register, i.e.

$$|\psi_i\rangle = \frac{|\widetilde{\psi_i}\rangle}{\sqrt{p_i}} \text{ if } p_i \neq 0, \text{ where } p_i = \langle\widetilde{\psi_i}|\widetilde{\psi_i}\rangle, \ |\widetilde{\psi_i}\rangle = E_{c,i}|\psi\rangle, \text{ and } 1 \leq i \leq k_c,$$

and then the following transition(s) is (are) implemented:

$$(c, |\psi\rangle) \to \{(c_i, |\psi_i\rangle) \mid p_i > 0, 1 \leq i \leq k_c\}.$$

Note that, the transitions having zero probability ($p_i = 0$) are not implemented.[12] The computation starts when the machine is in the initial classical configuration and the initial quantum state. The computation is terminated with the decision of "acceptance" ("rejection") if the machine enters an accepting (rejecting) configuration. The acceptance criteria of qATM is the same as ATM. For any given input, we have a computation tree representing all moves of the machine. The input is accepted if and only if there exists a *finite accepting subtree*[13] for a nondeterministic strategy in this computation tree. If we remove the work tape of a qATM, and restrict the input head to one-way, we obtain a one-way q-alternating finite automaton (q-1AFA).

We begin with a q-1AFA simulation of the qAM protocol given in the proof of Theorem 2. Thus, we obtain that q-alternation leads us to simulate any TM even the input head is restricted to one-way.

**Theorem 5.** *Any Turing-recognizable language can be recognized by a q-1AFA.*

*Proof.* Let L be a Turing-recognizable language, $\mathcal{D}$ be a single-tape DTM recognizing L, and $(P, V)$ be the qAM system for $L$, as described in the proof of Theorem 2. It is obvious that $V$ never needs to move its input head to the left in a single round. That is, the input head is used only at the beginning of each round to check whether the prover sends the valid initial configuration, which can be easily be implemented by moving the input head from the left to the right once. We define a new one-way finite state verifier $V'$ based on $V$. The only difference between $V$ and $V'$ is that when the outcome of an auxiliary operation element is observed, $V'$ terminates the computation with decision of "acceptance", instead of initiating a new round. Thus, $V'$ executes only a single round (and so $V'$ never needs to move its input head to the left).

The analysis of the proof system $(P, V')$ is as follows. Let $x$ be an input string. If $x \in$ L, the computation is terminated in every branch, and the input is accepted by $V'$ with probability 1 by the help of $P$. (Remember that $(P, V)$ has perfect-completeness.) If $x \notin$ L, there are two cases depending on the prover ($P^*$) strategy and also the behaviour of $\mathcal{D}$ on $x$: (1) the computation may be run forever in some branches, and, (2) the computation is terminated in every branch and the input is rejected by $V'$ with some non-zero probability .

Now, based on $V'$, we can easily construct a q-1AFA $\mathcal{A}$ recognizing L. The universal states of $\mathcal{A}$ simulate $V'$ and the existential states of $\mathcal{A}$ simulate the communications with all possible

[12] In terms of two-person games [Con89], we can say that *the player who makes the universal choices uses a quantum register to make its choices, therefore any choice with zero probability can never be a part of that player's strategy.*

[13] Each leaf of an accepting subtree is an accepting leaf, a leaf in which the decision of "acceptance" is given.

provers. If $x \in \mathtt{L}$, there exists a finite *accepting* subtree whose existential moves correspond to the communication with $P$. If $x \notin \mathtt{L}$, the finite sub-tree(s) can only be possible in the second case given above. Obviously, at least one leaf of such a subtree is a reject. Therefore, there is no finite accepting subtree for the nonmembers. □

**Corollary 4.** *For any space bound $s(n)$, q-1AFAs are strictly more powerful than any $s(n)$ space-bounded private ATM.*

*Proof.* This follows from Theorem 5 and the fact that the class of languages recognized by any space-bounded private ATM is a proper subset of decidable languages [Rei84], □

Since the entries of any operation element are rational numbers, any space-bounded qATM can be simulated by a DTM in a straightforward way. Due to this fact and Theorem 5, we cannot mention a space hierarchy for q-alternation. Moreover, the computation of qATMs may not be halted in some paths. Therefore, we define a restricted version of q-alternation: *strong q-alternation*. Any q-alternating machine is a strong one if it halts on every computational path. We will denote the related space complexity classes by $\mathsf{qASPACE}(\cdot)$, i.e. $\mathsf{qASPACE(s(n))}$ is the class of languages recognized by $s(n)$ space-bounded strong qATMs. $\mathsf{qAL}$ and $\mathsf{qAPSPACE}$ are strong q-alternating counterparts of $\mathsf{AL}$ and $\mathsf{APSPACE}$, respectively. We show that strong q-alternation (similar to private alternation [Rei84]) shifts the deterministic space hierarchy by exactly one level.

**Theorem 6.** *For any space-constructible $s(n) \in \Omega(\log(s(n)))$,*

$$\mathsf{DSPACE(2^{O(s(n))})} = \mathsf{qASPACE(s(n))}.$$

*Proof.* From [CKS81] and Lemma 3 (see below), we can follow that

$$\mathsf{DSPACE(2^{O(s(n))})} \subseteq \mathsf{ATIME(s(n))} \subseteq \mathsf{qASPACE(s(n))}.$$

From Lemma 2 (see below) and Savitch's theorem [Sav70], we can follow that

$$\mathsf{qASPACE(s(n))} \subseteq \mathsf{NSPACE(2^{O(s(n))})} \subseteq \mathsf{DSPACE(2^{O(s(n))})}.$$

□

**Corollary 5.** $\mathsf{L} \subsetneq \mathsf{qAL} = \mathsf{PSPACE} \subsetneq \mathsf{qAPSPACE} = \mathsf{EXPSPACE}$*.*

In the remaining part, we give some technical lemmata used in the proof of Theorem 6. We begin with showing an upper bound on the running time of a space-bounded strong qATM.

**Lemma 1.** *For any $s(n) \in \Omega(\log(n))$, the running time of a $s(n)$ space-bounded strong qATM can be at most $2^{O(s(n))}$.*

*Proof.* The proof follows from Appendix D. □

Due to Lemma 1, we can also provide a nondeterministic space simulation of a given space-bounded strong qATM by exponential blow-up.

**Lemma 2.** *For any space-constructible $s(n)$, if $\mathtt{L}$ is recognized by a $s(n)$ space-bounded strong qATM $\mathcal{A}$, there exists a $2^{O(s(n))}$ space-bounded NTM $\mathcal{N}$ recognizing $\mathtt{L}$.*

*Proof.* Let $x$ be a given input. The length of any computation path of $\mathcal{A}$ on $x$ can be at most $2^{c_1 s(|x|)}$ and any configuration length can be at most $c_2 s(|x|)$, for appropriate numbers $c_1$ and $c_2$. We know that if $x \in \mathtt{L}$, there exists a nondeterministic strategy that leads to an accepting subtree, and, if $x \notin \mathtt{L}$, the subtree of each nondeterministic strategy has at least one rejecting leaf (a leaf in which the decision of "rejection" is given). $\mathcal{N}$ nondeterministically implements each strategy of $\mathcal{A}$ on $x$, and, for each strategy, traces the corresponding subtree path-by-path by using $2^{O(s(|x|))}$ space. Note that $2^{O(s(|x|))}$ space is also sufficient to trace the content of the quantum register in a path since in each step, the precision of any amplitude can be increased by at most a constant, and so the space to hold the state of the register increases at most by a constant in each step.

If $\mathcal{N}$ detects a rejecting leaf for a strategy, then it rejects the input. If there is no such a leaf for a strategy, then it accepts the input. Therefore, if $x \in \mathtt{L}$, $\mathcal{N}$ accepts the input in at least one of its nondeterministic branch; and, if $x \notin \mathtt{L}$, the input is rejected in all nondeterministic branches. □

Now, we show that the bound given in Lemma 2 is actually tight.

**Lemma 3.** *For any log-space constructible $t(n) \in \Omega(n)$, if $L$ is recognized by a ATM $\mathcal{A}$ running in time $t(n)$, then there exists a $O(\log(t(n)))$ space-bounded strong qATM $\mathcal{A}'$ recognizing $L$.*

*Proof.* We know that any $s(n)$ space-bounded ATM can be simulated by a $O(\log(s(n)))$ space-bounded qAM proof system, say $(P, V)$, with perfect-completeness (Theorem 4). A generic schema of this simulation is as follows:

```
BEGIN LOOP
   $V$ obtains a computation path of the ATM on the given input from the prover
   $V$ processes this computation and makes a decision with some probability
   IF $V$ makes a decision, THEN the computation (LOOP) is terminated
END LOOP
```

Let $x$ be an input. In this simulation, $V$ can deterministically check weather the length of of a configuration sent by the prover is $cs(|x|)$ by using its work tape, where $c$ is an appropriate number. On the other hand, the maximum length of a single-round is determined by the prover. For example, for a valid computation, a honest prover can send $2^{O(s(|x|))}$ configurations, and $V$ can only count until $O(s(|x|))$ by using a "standard" counter.

If we replace the simulated ATM with our $t(n)$ time-bounded ATM $\mathcal{A}$, then the same protocol can still work with space bound $O(\log(t(n)))$. Now, the maximum length of a single-round can be determined by the verifier since it can count $t(|x|)$ in this case and can terminate the computation with decision of "rejection" if the prover does not sent a halting configuration of $\mathcal{A}$ until then. We denote this new proof system as $(P', V')$. By using the idea given in the proof of Theorem 5, we can define a new verifier $V''$ based on $V'$ such that it terminates the computation with the decision of "acceptance" when it observes the outcome of an auxiliary operation element, and so it implements only a single-round of $(P', V')$.

The analysis of the proof system $(P', V'')$ is as follows. The computation is terminated in every branch. If $x \in \mathtt{L}$, it is accepted by $V''$ with probability 1 (due to perfect-completeness) by the help of $P'$. If $x \notin \mathtt{L}$, the input is always rejected by $V'$ with some non-zero probability.

As described in the proof of Theorem 5, we can easily construct a $O(\log(t(|x|)))$ space-bounded qATM $\mathcal{A}'$ based on $V''$, which recognizes $\mathtt{L}$: The universal states of $\mathcal{A}'$ simulate $V''$, and the existential states of $\mathcal{A}$ simulate the communications with all possible provers. If $x \in \mathtt{L}$, there exists a finite *accepting* subtree whose existential moves correspond to the communication with $P'$. If $x \notin \mathtt{L}$, any finite subtree contains at least one rejecting leaf. □

**Acknowledgements.** We would like to thank Andris Ambainis and A. C. Cem Say for their many helpful comments on some drafts of this paper.

# A A review of previous private protocols

In this part, we review the private protocols for obtaining the results given in Facts 2 and 3, which we will refer as *the weak-protocol* and *the strong-protocol*, respectively. (Since Fact 4 is a generalization of Fact 3 [DS92], we omit its details.) The main idea behind both protocols for a given language is to simulate a fixed machine recognizing the given language: The prover sends to the verifier the computation of the simulated machine on a given input, which is a sequence of configurations starting from the initial configuration, and the verifier tries to verify the correctness of this sequence and then gives a decision with respect to the halting configuration sent by the prover. During the verification procedure, the following tasks can easily be checked deterministically: (i) each configuration has a correct format, and (ii) the sequence starts with the initial configuration and ends with a halting configuration. In the latter protocol, the length of each configuration is also checked to be at most linear. On the other hand, to check whether the prover sends a valid next configuration after each one is a non-trivial task. We will call this task *successor-check* and this is indeed where the private coin-flips come into play.

Since a single computation requires many adjunctive successor-checks and each of them contains many (private) coin-flips, a decision on the input can only be given with a very small probability after passing a single computation. Therefore, the prover sends the computation repeatedly in an infinite loop. Depending on the machine and resources of the the verifier, either the verifier can always halt the computation with high probability or the protocol can run forever in some cases. For example, if the simulated machine never halts on the input and the prover honestly sends the corresponding computation, the verifier can never halt and give a decision.

Now, we give some protocol specific details. We begin with the weak-protocol of Condon and Lipton [CL89]. In his seminal paper [Fre81], Freivalds presented a two-way probabilistic finite automaton (pfa) recognizing language

$$\mathtt{FRE} = \{a^{n_1}b^{n_1}a^{n_2}b^{n_2}\cdots a^{n_k}b^{n_k} \mid n_1,\ldots,n_k > 0, k > 0\}$$

with bounded error. Based on Freivalds' algorithm, Condon and Lipton proposed a private protocol such that if a prover sends a member of FRE repeatedly to a one-way pfa verifier, then the verifier detects the memberships of the input with high probability. If the prover sends some nonmembers of FRE repeatedly to the same verifier, then the verifier gives a decision of rejection with high probability. Two-way finite automata with two-counters (2D2CA) are Turing-equivalent [Min67], and their main configuration elements are the contents of the counters, which can be encoded unary. Then successor-checks on a computation of a 2D2CA can be implemented by the protocol given by Condon and Lipton. Let L be a Turing-recognizable language and $\mathcal{D}$ be the 2D2CA recognizing it. For the members of L, the (honest) verifier sends finite valid configurations, and so the verifier accepts the input them with high probability. For the nonmembers of L, the verifier can only accept if the last configuration of the computation is an accepting one. This means that the computation contains at least one defect, and so the probability of rejection is greater than the probability of acceptance due to the defect. Since a prover can never sends a halting configuration, the protocol has a weak-soundness.

In the case of the strong-protocol of Dwork and Stockmeyer [DS92], the simulated machine is an $O(n)$ space-bounded ATM, say $\mathcal{A}$. In order to simplify the proof, some inessential assumptions are made on $\mathcal{A}$: Roughly, each existential or universal transition leads to exactly two branches, there is no consecutive two existential or universal branching, $\mathcal{A}$ uses only $|x| + 2$ space, $\mathcal{A}$ always halts exactly after $2^{c|x|}$ branching steps by keeping a counter, and so $\mathcal{A}$ never enters a loop, where $x$ is a given input and $c$ is an appropriate constant. Note that the computation tree of $\mathcal{A}$ on $x$ has $2^{2^{c|x|}}$ leafs. The prover repeatedly sends the computation of some paths of this tree, in which the nondeterministic choices are made by the prover and the universal choices are made by the verifier, i.e. the verifier flips a coin and sends the outcome to the verifier. The configurations on a computation are separated by \$'s as

$$\cdots \$ c_i \$ c_{i+1} \$ c_{i+2} \$ \cdots ,$$

where $i > 0$. Since each configuration of $\mathcal{A}$ on $x$ is fixed length ($|x| + 3$), the verifier can implement the successor-check by deterministically comparing the symbols at distance $|x| + 4$ by using its input head.[14] If there is not exactly one \$ between two symbols, then the input is rejected by the verifier. The private part of the successor-check is that the verifier always selects the first symbol randomly and repeats this selection after each comparison. That is, if $l > 0$ is the index of a selected symbol, then it is compared with $(l + |x| + 4)^{th}$ symbol, and then a new symbol with an index between $(l + |x| + 4) + 1$ and $(l + |x| + 4) + |x| + 4$ is selected. Since the protocol is private, the prover can never know which two symbols are compared. Thus, any defect on the computation can always be detected by the verifier with some probability, which is sufficiently greater than any accept probability. If there is no defect, the accepting probability is still very small so that a single rejecting probability on a leaf can always dominate the cumulative accepting probabilities from all the other leafs. (We omit the details here but the same issue is also detailed in the proof of Theorem 3.) Therefore, for the strings accepted by $\mathcal{A}$, none of successor-check produces a rejecting probability, and so the verifier accepts the input exactly by help of a honest prover. For the strings rejected by $\mathcal{A}$, if the input is not rejected by any successor-check, the input is rejected at least one path which is sufficient to dominate all the accepting decisions. Note that, if the prover never sends a halting configuration, the verifier detects infinitely many defects, which are sufficient to reject the input with probability 1, by using its input head.

As seen from the details, the private methods used by the protocols are different. In the former one, the verifier privately collects statistical evidence from over the computations to decide their correctness. Moreover, two-sided error is necessary in this case due to Theorem 1. In the latter case, the verifier can force the prover to send linear size configurations and then detects the defects directly. The latter protocol has also perfect-completeness.

## B The proof of Theorem 1

The proof of $\mathsf{IP_1(s(n))} \subseteq \mathsf{weak\text{-}IP_1(s(n))} \subseteq \mathsf{ASPACE}(2^{2^{O(s(n))}})$ follows from Lemma 4 (see below) and [CKS81], where $s(n) \in \Omega(\log(n))$ is space-constructible.

We begin with a definition: The prover-verifier pair $(P, V)$ is an *unbounded-error IPS having perfect completeness* for $L$ if it has a perfect-completeness, i.e. satisfying condition $(1')$, and has the following soundness condition:

$2''$. for all $x \notin L$, and all provers $P^*$, the probability that $(P^*, V)$ accepts $x$ is less than 1.

The classes defined by unbounded-error IPS having perfect completeness will be shown by $\mathsf{IP}_{1,<1}(\cdot)$.

**Lemma 4.** *For any space-constructible $s(n) \in \Omega(\log(n))$,*

$$\mathsf{IP_{1,<1}(s(n))} \subseteq \mathsf{DSPACE}(2^{2^{2^{O(s(n))}}}).$$

[14] If the simulated machine is $s(n) \in \omega(n)$ space-bounded, then $\log(s(n))$ space-bounded verifier is sufficient for a similar check, where $s$ is a space-constructible function.

*Proof.* Let $\mathtt{L} \in \mathsf{IP}_{1,<1}(\mathsf{s(n)})$. Then there exists an unbounded-error IPS having perfect-completeness $(P, V)$ for $\mathtt{L}$. We will show that a DTM can recognize $\mathtt{L}$ by using triple-exponential time in $s(n)$.

Let $x$ be an input string. Without loss of generality, we assume that the communication alphabet contains exactly two symbols $\{0, 1\}$. We represent the configuration set of $V$ on $x$ as $\mathcal{C}_V(x)$, whose size is exponential in $s(|x|)$. We classify the configurations into five groups:

1. `read`: the ones in a reading state

2. `comm-0`: the ones in a communication state ready to write 0 on the communication cell

3. `comm-1`: the ones in a communication state ready to write 1 on the communication cell

4. `acc`: the ones in an accepting state

5. `rej`: the ones in a rejecting state

The computation tree of $(P', V)$ on $x$ can be infinite for a prover $P'$. On the other hand, *having perfect completeness* allow us to build a finite computation tree that concisely represents the computation of $V$ on $x$ and its communications with all possible provers ($P^*$). First of all, we do not need to keep the probabilities of the configurations since the input is either accepted with probability 1 or with a probability less than 1. (We do not need the cumulative sums of the accepting and rejecting probabilities.) Secondly, the length of any halting path must be bounded by a certain number steps. If the computation does not halt, then $V$ must enter an infinite loop. An infinite loop, *in our case*, can either contributes to a halting path or independent from the other parts of the computation. We visualize both cases in Figure 2. The former case can be seen as a part of the halting path since the probability of being in the loop approaches to zero and the halting path is re-traversed with the decreasing probability after each cycle. However, the probability of being in the loop remains the same in latter case, and so it should be replaced with a rejecting path if detected.

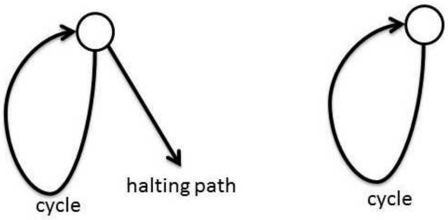

Figure 2: Two cases of infinite loops

We denote our finite tree $\mathcal{T}_V(x)$. (Note that we do not specify any prover since this tree represent all possible communication scenarios.) The structure and evaluation of $\mathcal{T}_V(x)$ is similar to the computation tree of an ATM. The main difference of $\mathcal{T}_V(x)$ is that a node can take three different values instead of two values, which are originally true and false. We give the details of how $\mathcal{T}_V(x)$ can be constructed below.

Since the protocol is private, we keep the configurations that follow the same communication strategy together. Therefore, each node of $\mathcal{T}_V(x)$ represents a subset of $\mathcal{C}_V(x)$. The root represents the initial configuration. We have four different types of inner nodes, i.e.

$$\textsc{read-comm}, \textsc{comm-}01, \textsc{comm-}0, \text{ and } \textsc{comm-}1,$$

and three different types of leafs, i.e.

ACC, REJ, and LOOP.

A READ-COMM node, say RC, is a node that contains at least one `read` configuration and may contain some `comm-0` or `comm-1` configurations. The child node(s) of RC is (are) determined as follows: Each `read` configuration in RC divides into at most two child configurations in a single step.

- If the child is an `acc` (a `rej`) configuration, then an ACC (a REJ) leaf is created and connected to the RC.
- If the child is a `read` configuration which is identical to a `read` configuration in RC, then a LOOP leaf is created and connected to RC.
- In any other case, each child should be one of a `read` (not in RC), a `comm-0`, or a `comm-1` configuration. All these children with the previous `comm-0` or `comm-1` configurations form a new node and connected to RC.

The type of the new node given in the last item is determined conditionally. If its depth (in $\mathcal{T}_V(x)$) exceeds a certain number ($2^{|\mathcal{C}_V(x)|}$ – the total number of all subsets of $\mathcal{C}_V(x)$), it becomes a LOOP leaf since it must be a repetition of a previous node along the same path.

Suppose that the depth of the new node does not exceed this number. If it contains at least one `read` configuration, then it becomes a READ-COMM node again. If it contains both `comm-0` and `comm-1` configurations, then it becomes a COMM-01 node. If it contains only some `comm-0` (`comm-1`) configurations, then it becomes a COMM-0 (COMM-1) node.

For each COMM-01 node, say C01, two new nodes are created and connect to C01. One of them becomes a COMM-0 node that contains all `comm-0` configurations of C01. The other one becomes a COMM-1 node that contains all `comm-1` configurations of C01. Both COMM-0 and COMM-1 are the communication nodes. We give the details for a COMM-0, say C0, node. (The situation is exactly the same for a COMM-1 node.) Let $c$ be a configuration in C0. In $c$, the verifier writes 0 on the communication cell, and then receives 0 or 1. Since we consider all possible communications, there are two next configurations evolved from $c$ in a single step, say $c_0$ and $c_1$. If $c_0$ ($c_1$) is an `acc` or a `rej` configuration, then an ACC or a REF leaf is created, respectively, and connected to the C0; or if $c_0$ ($c_1$) is a `comm-0` configuration which is identical to a `comm-0` configuration in C0, then a LOOP leaf is created and connected to C0. Otherwise, all $c_0$'s and $c_1$'s are collected into two new nodes and then connected to C0. The types of the new nodes are determined as explained above. We completed how $\mathcal{T}_V(x)$ can be constructed.

Now, we describe how $\mathcal{T}_V(x)$ can be evaluated. We associate each inner node with "$\wedge$" or "$\vee$" operator: READ-COMM and COMM-01 are associated with "$\wedge$" (universal choice), and COMM-0 and COMM-1 are associated with "$\vee$" (nondeterministic choice). These operators determines the value of a node from the values of its children. There are three types of values: true, false, and loop[depth], where depth is a numeric value. Obviously, any ACC (REJ) leaf takes the value of true (false). Any LOOP leaf takes the value of loop with a depth value that represent the smallest depth of the repeated node.

If the computation tree just contains true and false values, then its evaluation becomes trivial (exactly the same as alternation). The non-trivial part is how to include the loop into the evaluation. Suppose that a node associated with "$\wedge$" has $k > 0$ child/children, whose values are represented by $v_1, \ldots, v_k$. The value of the node can be calculated as follows:

$$v_1 \wedge (v_2 \wedge \cdots (v_{k-2} \wedge (v_{k-1} \wedge v_k))),$$

where binary relation "$\wedge$" is defined as follows:

| $\wedge$ | true | false | loop[$\mathsf{d}_1$] |
|---|---|---|---|
| true | true | false | true |
| false | false | false | false |
| loop[$\mathsf{d}_2$] | true | false | loop[$min\{\mathsf{d}_1, \mathsf{d}_2\}$] |

Since it is a universal choice, any false value beats all the other values. Any true value beats any loop value, since this loop contributes the accepting path. Between two loop values, we select the one having smaller depth. The value of a "$\vee$" node can be calculated in a similar way with its specific rules:

| $\vee$ | true | false | loop[$\mathsf{d}_1$] |
|---|---|---|---|
| true | true | true | true |
| false | true | false | loop[$\mathsf{d}_1$] |
| loop[$\mathsf{d}_2$] | true | loop[$\mathsf{d}_2$] | loop[$min\{\mathsf{d}_1, \mathsf{d}_2\}$] |

Since it is an existential (nondeterministic) choice, any true value beats all the other values. Any loop value beats any false value, since the corresponding loop may contribute an accepting path in a lower depth. Between two loop values, we again select the one having smaller depth. The last thing about the evaluation is that if a node takes value of loop and the depth of the loop refers to this node, then the value of the node is changed to false since this loop does not contribute any accepting path. The value of the root is the value of the tree.

In case of $x \in \mathtt{L}$, we know that there exists a nondeterministic strategy (corresponding to the communication with $P$) on the tree such that it does not lead to any rejecting path, and any infinite loop must contribute some accepting paths. Therefore, the value of the root is set to true.

In case of $x \notin \mathtt{L}$, we know that for every nondeterministic strategy (corresponding to the communication with $P^*$), there must be a nonzero rejecting path or a nonzero looping path (not contributing any accepting path) that dominates all the other opponent values during the evaluation. Therefore, the value of the root is set to false.

A DTM can construct and evaluate $\mathcal{T}_V(x)$ in a straightforward way. Since the depth of the tree is $2^{|\mathcal{C}_V(x)|}$, the total running time of the DTM is double-exponential in $|\mathcal{C}_V(x)|$. Since $|\mathcal{C}_V(x)|$ is exponential in $s(|x|)$, then the total running time becomes triple-exponential in $s(|x|)$. □

# C A constant-space qAM protocol for SUBSET-SUM

In this appendix, we present a qAM system having a finite-state verifier for the well-known NP-complete language SUBSET-SUM, which is the collection of all strings of the form $S\$a_1\$\ldots\$a_n\$$ such that $S$ and the $a_i$'s are numbers in binary ($1 \leq i \leq n$), and there exists a set $I \subseteq \{1,\ldots,n\}$ satisfying $\sum_{i\in I} a_i = S$, where $n > 0$.

**Lemma 5.** SUBSET-SUM $\in$ qAM(1).

*Proof.* We assume that the input to be of the form $S\$a_1\$\ldots\$a_n\$$, where $S$, the $a_i$'s are numbers in binary ($1 \leq i \leq n$), and $n > 0$. (If not, the input is immediately rejected.) The input is written between two # symbols on the input tape and its head is not allowed to cross these boundaries.

The main idea is that the verifier scans the input from left to right in an infinite loop and firstly encodes $S$, and then subtracts the encoding of each of the $a_i$'s selected by the prover, in some amplitudes of the states on the quantum register. And at the end of the loop (round), the verifier tests whether the result is zero or not (described later). Since our encoding procedure works by reducing the amplitude with a constant in each step, the process can successfully be ended with an exponentially small probability depending on the length of the input. Therefore, a new round is initiated with remaining huge probability.

The register has 3 states, $\{q_1, q_2, q_3\}$. Each round is composed by five parts, described below. The details of superoperators applied in each round are given in Figure C, where each outcome is given under the operation element. The actions associated to each outcome are as follows: (i) The input head is moved forward if outcome "$f$" is observed, (ii) the input is accepted (rejected) if outcome "$a$" ("$r$") is observed, and (iii) a new round is initiated if outcome "$i$" is observed.

1. The finite register is initialized on symbol #: $|\psi_0\rangle = (1\ \ 0\ \ 0)^T$.
2. $S$ is encoded into the amplitudes of $|q_2\rangle$: $\mathcal{E}_\sigma$ is applied on the quantum register when reading $\sigma \in \{0,1\}$. Then, $\mathcal{E}_\$$ is applied on the quantum register when reading \$.
3. Each $a_i$ $(1 \leq i \leq n)$ is encoded into the amplitude of $|q_3\rangle$: $\mathcal{E}'_\sigma$ is applied on the quantum register when reading $\sigma \in \{0,1\}$.
4. If an $a_i$ $(1 \leq i \leq n)$ is *selected* by the prover on symbol \$, it is subtracted from the number represented by the amplitude of $|q_2\rangle$: $\mathcal{E}'{}_\$$ is applied on the quantum register. If it is not selected, $\mathcal{E}''_\$$ is applied on the quantum register. Note that, the amplitude of $|q_3\rangle$ is set to 0 after each of these transformations.
5. The decision is given on #: $\mathcal{E}_\#$ is applied on the quantum register when reading #.

| | |
|---|---|
| Part 2: | $\mathcal{E}_0=\left\{\underbrace{\frac{1}{3}\begin{pmatrix}1&0&0\\0&2&0\\0&0&1\end{pmatrix}}_{f},\underbrace{\frac{1}{3}\begin{pmatrix}2&0&-2\\2&0&2\\0&2&0\end{pmatrix}}_{i},\underbrace{\frac{1}{3}\begin{pmatrix}0&1&0\\0&0&0\\0&0&0\end{pmatrix}}_{i}\right\},\ \mathcal{E}_1=\left\{\underbrace{\frac{1}{3}\begin{pmatrix}1&0&0\\1&2&0\\0&0&1\end{pmatrix}}_{f},\underbrace{\frac{1}{3}\begin{pmatrix}2&-1&0\\1&0&2\\1&0&-2\end{pmatrix}}_{i},\underbrace{\frac{1}{3}\begin{pmatrix}1&0&0\\0&2&0\\0&0&0\end{pmatrix}}_{i}\right\}$ |
| Part 2: | $\mathcal{E}_\$=\left\{\underbrace{\frac{1}{3}\mathcal{I}}_{f},\underbrace{\frac{1}{3}2\mathcal{I}}_{i},\underbrace{\frac{1}{3}2\mathcal{I}}_{i}\right\}$ |
| Part 3: | $\mathcal{E}'_0=\left\{\underbrace{\frac{1}{3}\begin{pmatrix}1&0&0\\0&1&0\\0&0&2\end{pmatrix}}_{f},\underbrace{\frac{1}{3}\begin{pmatrix}2&2&0\\2&-2&0\\0&0&2\end{pmatrix}}_{i},\underbrace{\frac{1}{3}\begin{pmatrix}0&0&1\\0&0&0\\0&0&0\end{pmatrix}}_{i}\right\},\ \mathcal{E}'_1=\left\{\underbrace{\frac{1}{3}\begin{pmatrix}1&0&0\\0&1&0\\1&0&2\end{pmatrix}}_{f},\underbrace{\frac{1}{3}\begin{pmatrix}2&0&-1\\1&2&0\\1&-2&0\end{pmatrix}}_{i},\underbrace{\frac{1}{3}\begin{pmatrix}1&0&0\\0&0&2\\0&0&0\end{pmatrix}}_{i}\right\}$ |
| Part 4: | $\mathcal{E}'_\$=\left\{\underbrace{\frac{1}{3}\begin{pmatrix}1&0&0\\0&1&-1\\0&0&0\end{pmatrix}}_{f},\underbrace{\frac{1}{3}\begin{pmatrix}0&-1&1\\2&1&-1\\2&-1&1\end{pmatrix}}_{i},\underbrace{\frac{1}{3}\begin{pmatrix}0&2&2\\0&0&0\\0&0&0\end{pmatrix}}_{i},\underbrace{\frac{1}{3}\begin{pmatrix}0&1&0\\0&0&1\\0&0&0\end{pmatrix}}_{i}\right\},\ \mathcal{E}''_\$=\left\{\underbrace{\frac{1}{3}\begin{pmatrix}1&0&0\\0&1&0\\0&0&0\end{pmatrix}}_{f},\underbrace{\frac{1}{3}\begin{pmatrix}2&-2&0\\2&2&0\\0&0&3\end{pmatrix}}_{i}\right\}$ |
| Part 5: | $\mathcal{E}_\#=\left\{\underbrace{\frac{1}{3}\begin{pmatrix}1&0&0\\0&0&0\\0&0&0\end{pmatrix}}_{a},\underbrace{\frac{1}{3}\begin{pmatrix}0&0&0\\0&3&0\\0&0&0\end{pmatrix}}_{r},\underbrace{\frac{1}{3}\begin{pmatrix}2&0&0\\2&0&0\\0&0&3\end{pmatrix}}_{i}\right\}$ |

Figure 3: The details of superoperators used by the qAM system for `SUBSET-SUM`

Let $w$ be the input and $T$ be the cumulative sum of selected $a_i$'s by the prover. Then, the state of the register before reading # becomes

$$|\widetilde{\psi_{|w|}}\rangle = \left(\frac{1}{3}\right)^{|w|}\begin{pmatrix}1\\S-T\\0\end{pmatrix}.$$

After applying $\mathcal{E}_\#$, the input is rejected with probability

$$\left(\frac{1}{3}\right)^{2|w|+2}(3S-3T)^2,$$

which is at least $9\left(\frac{1}{3}\right)^{2|w|+2}$ if $S \neq T$ and is exactly equal to 0 if $S = T$. On the other hand, the input is always accepted with probability $\left(\frac{1}{3}\right)^{2|w|+2}$. Therefore, if $w \in \texttt{SUBSET-SUM}$, there exists a prover such that it is accepted exactly, and if $w \notin \texttt{SUBSET-SUM}$, whatever the prover says, it is rejected with a probability at least $\frac{9}{10}$. The error bound can be reduced to any desired value by using probability amplification. □

# D A time-bound for absolutely-halting space-bounded quantum Turing machines

The first space-bounded QTM model was introduced by Watrous [Wat98, Wat99b], and he showed that any such $s(n)$ space-bounded QTM that always halts on every input can run at most $2^{O(s(n))}$ steps, where $s(n) \in \Omega(\log(n))$. Since the nonhalting part of such a model can always be in a single pure (quantum) state, the same result cannot be directly applicable to the QTMs whose halting part can be in a mixture of some pure states (mixed-state). The qATM introduced in Section 4 and the models introduced in [Wat03, YS11b, vMW12] are some examples for the latter case.

On the other hand, since any mixed-state and the operator(s) applied to it can be represented by a single vector and a single matrix, respectively, the result given by Watrous can be extended to general case. We will provide an explicit proof of this result below.

A QTM can have both classical and quantum parts. Let $\mathcal{M}$ be such a space-bounded QTM and $x$ be an input. A standard configuration of $\mathcal{M}$ on $x$ is a pair of $(c, |d\rangle)$, where $c$ is a configuration of the classical part and $|d\rangle$ is a (standard) basis vector of the quantum part. During the computation, $\mathcal{M}$ can be in some mixture of $(c, |\psi\rangle)$'s, where each $|\psi\rangle$ can be either a basis vector or a superposition of some basis vectors.

**Theorem 7.** *Let $N$ be the number of the standard configurations of an absolutely-halting space-bounded QTM $\mathcal{M}$ on a given input $x$. Then, $\mathcal{M}$ can run at most $N^2$ steps on $x$.*

*Proof.* In space-bounded quantum computation, the computation is regularly observed whether it is terminated or continued, and then the observed part is normalized. The nonhalting part of $\mathcal{M}$ on $x$ can be represented by an $N \times N$-dimensional density matrix. Since we consider whether this matrix is equal to zero matrix or not, we can omit the normalization part. Based on the local transitions of $\mathcal{M}$, we can defined some finite, say $k$, $N \times N$ matrices $\{E_1, \ldots, E_k\}$ that represent one step transformation of the nonhalting part. Thus, we obtain the following matrix sequence that represent the nonhalting part for each step:

$$\nu_0, \nu_1, \nu_2, \ldots \ , \tag{4}$$

where $\nu_0$ is the initial one and $\nu_i$ represents the $i^{th}$ $(i > 0)$ one obtained after $i^{th}$ steps, which is calculated as:

$$\nu_i = \sum_{j=1}^{k} E_j \nu_{i-1} E_j^{\dagger}.$$

If $\mathcal{M}$ halts on every input absolutely, there must be an index $i'$ such that $\nu_{i'} = 0$. As pointed out above, the sequence given in Eq. 4 can be represented by vectors, and each of them (except the initial one) can be obtained by applying a single operator (matrix) to the previous vector in the sequence. That is, based on $\nu_0$ and $\{E_1, \ldots, E_k\}$, we define an $N^2$-dimensional vector, say $v_0$, and $N^2 \times N^2$-dimensional matrix, say $E$, respectively, and then Eq. 4 turns out be as follows:

$$v_0, v_1, v_2, \ldots \ ,$$

where

$$v_i = Ev_{i-1} \quad (i > 0).$$

We refer the reader to Page 73 of [Wat03] for the details of this conversion. Now, we will show that $i'$ cannot be bigger than $N^2$ due to the following fact.

**Fact 6.** *For any $m$-dimensional vector $u$, if $A^m u \neq 0$, then $A^{m+j} u \neq 0$, where $A$ is an $m \times m$-dimensional matrix and $j > 0$.*[15]

*Proof.* The proof can be easily obtained from the following well-known relation:

$$ker(A) \subseteq ker(A^2) \subseteq \cdots \subseteq ker(A^m) = ker(A^{m+1}) = ker(A^{m+2}) = \cdots$$

That is, if $u$ is not in $ker(A^m)$, then $u$ cannot be in $ker(A^{m+j})$ for any $j > 0$. □

Thus we can say that if $Ev_{N^2} \neq 0$, then $v_{N^2+j}$ cannot be equal to zero for any $j > 1$, i.e. $\mathcal{M}$ cannot halt absolutely on $x$. Therefore, $i'$ cannot be bigger than $N^2$, which is a quadratic bound in terms of the number of configurations. □

**Corollary 6.** *Any $s(n) \in \Omega(\log(n))$ space-bounded QTM that always halt on every input can run at most $2^{O(s(n))}$ steps.*

## References

[AN02] Dorit Aharonov and Tomer Naveh. Quantum NP – A survey. Technical report, 2002. arXiv:0210077.

[AW02] Andris Ambainis and John Watrous. Two–way finite automata with quantum and classical states. *Theoretical Computer Science*, 287(1):299–311, 2002.

[Bab85] László Babai. Trading group theory for randomness. In *STOC'85: Proceedings of the 17th Annual ACM Symposium on Theory of Computing*, pages 421–429, 1985.

[CHPW98] Anne Condon, Lisa Hellerstein, Samuel Pottle, and Avi Wigderson. On the power of finite automata with both nondeterministic and probabilistic states. *SIAM Journal on Computing*, 27(3):739–762, 1998.

[CKS81] Ashok K. Chandra, Dexter C. Kozen, and Larry J. Stockmeyer. Alternation. *Journal of the ACM*, 28(1):114–133, 1981.

[CL88] Anne Condon and Richard E. Ladner. Probabilistic game automata. *Journal of Computer and System Sciences*, 36(3):452–489, 1988.

[CL89] Anne Condon and Richard J. Lipton. On the complexity of space bounded interactive proofs (extended abstract). In *FOCS'89: Proceedings of the 30th Annual Symposium on Foundations of Computer Science*, pages 462–467, 1989.

[Con89] Anne Condon. *Computational Models of Games*. MIT Press, 1989.

[Con91] Anne Condon. Space-bounded probabilistic game automata. *Journal of the ACM*, 38(2):472–494, 1991.

[15] Observe that one can easily find an example of $A$ and $u$ such that $A^{m-1}u \neq 0$ but $A^m u = 0$.

[Con93] Anne Condon. *Complexity Theory: Current Research*, chapter The complexity of space bounded interactive proof systems, pages 147–190. Cambridge University Press, 1993.

[CS76] Ashok K. Chandra and Larry J. Stockmeyer. Alternation. In *FOCS'76: Proceedings of the 17th IEEE Symposium on Foundations of Computer Science*, pages 98–108, 1976.

[DS92] Cynthia Dwork and Larry Stockmeyer. Finite state verifiers I: The power of interaction. *Journal of the ACM*, 39(4):800–828, 1992.

[Fre81] Rūsiņš Freivalds. Probabilistic two-way machines. In *Proceedings of the International Symposium on Mathematical Foundations of Computer Science*, pages 33–45, 1981.

[GMR85] Shafi Goldwasser, Silvio Micali, and Charles Rackoff. The knowledge complexity of interactive proof-systems (extended abstract). In *STOC'85: Proceedings of the 17th Annual ACM Symposium on Theory of Computing*, pages 291–304, 1985.

[GMR89] Shafi Goldwasser, Silvio Micali, and Charles Rackoff. The knowledge complexity of interactive proof systems. *SIAM Journal on Computing*, 18(1):186–208, 1989.

[JJUW11] Rahul Jain, Zhengfeng Ji, Sarvagya Upadhyay, and John Watrous. QIP = PSPACE. *Journal of the ACM*, 58(6):30, 2011.

[Kit99] Alexei Kitaev. Quantum NP, January 1999. Talk at AQIS'99: Second Workshop on Algorithms in Quantum Information Processing.

[Kni96] Emanuel Knill. Quantum randomness and nondeterminism. Technical Report arXiv:quant-ph/9610012, 1996.

[Koz76] Dexter C. Kozen. On parallelism in Turing machines. In *FOCS'76: Proceedings of the 17th IEEE Symposium on Foundations of Computer Science*, pages 89–97, 1976.

[Min67] Marvin Minsky. *Computation: Finite and Infinite Machines.* Prentice-Hall, 1967.

[MW05] Chris Marriott and John Watrous. Quantum Arthur-Merlin games. *Computational Complexity*, 14(2):122–152, 2005.

[NY09] Harumichi Nishimura and Tomoyuki Yamakami. An application of quantum finite automata to interactive proof systems. *Journal of Computer and System Sciences*, 75(4):255–269, 2009.

[Pap85] Christos H. Papadimitriou. Games against nature. *Journal of Computer and System Sciences*, 31(2):288–301, 1985.

[Rei84] John H. Reif. The complexity of two-player games of incomplete information. *Journal of Computer and System Sciences*, 29(2):274–301, 1984.

[Sav70] Walter J. Savitch. Relationships between nondeterministic and deterministic tape complexities. *Journal of Computer and System Sciences*, 4(2):177–192, 1970.

[Sha92] Adi Shamir. IP = PSPACE. *Journal of the ACM*, 39(4):869–877, 1992.

[vMW12] Dieter van Melkebeek and Thomas Watson. Time-space efficient simulations of quantum computations. *Theory of Computing*, 8(1):1–51, 2012.

[Wat98] John Watrous. *Space-bounded quantum computation*. PhD thesis, University of Wisconsin - Madison, USA, 1998.

[Wat99a] John Watrous. PSPACE has constant-round quantum interactive proof systems. In *FOCS'99: Proceedings of the 40th Annual Symposium on Foundations of Computer Science*, pages 112–119, 1999.

[Wat99b] John Watrous. Space-bounded quantum complexity. *Journal of Computer and System Sciences*, 59(2):281–326, 1999.

[Wat03] John Watrous. On the complexity of simulating space-bounded quantum computations. *Computational Complexity*, 12(1-2):48–84, 2003.

[YS10] Abuzer Yakaryılmaz and A. C. Cem Say. Languages recognized by nondeterministic quantum finite automata. *Quantum Information and Computation*, 10(9&10):747–770, 2010.

[YS11a] Abuzer Yakaryılmaz and A. C. Cem Say. NP has log-space verifiers with fixed-size public quantum registers. Technical Report arXiv:1101.5227, 2011.

[YS11b] Abuzer Yakaryılmaz and A. C. Cem Say. Unbounded-error quantum computation with small space bounds. *Information and Computation*, 279(6):873–892, 2011.